International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 3, May 2014, 167-170

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

PECULIARITY BASED ENCRYPTION

SHIKHA SINGH[1] & HARPREET SINGH CHAWLA[2]

[1]Research Scholar, Institute of Foreign Trade and Management University, Moradabad, Uttar Pradesh, India

[2]Assistant Professor, IFTM University, Moradabad, Uttar Pradesh, India

ABSTRACT

As the technology changes, there is also a need to define and view the concepts of security under various dimensions. Recent dimension of security is the peculiarity based view that has been conceived by the requirements in a distributed setting. Signature schemes have been developed in order to give a more fine grained access control. This mechanism is useful is useful in settings where the list of users may not be known apriori users may possess some credentials and these are used to determine access control and also provide a reasonable degree of anonymity with respect to the user's identity Cipher text based encryption is a scheme that gives a way to separate the credentials from the access policy and cleverly combine them at a later stage to provide secure access to protected data. In schemes the size of the cipher text is quite large and is of the order of the number of attributes. In this we present our approach for a multi-level threshold based encryption which is independent of the number of attributes.

KEYWORDS: Setup, Encrypt, Key Generation Y Decrypt, As Described Next

INTRODUCTION

It is a type of encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, we can decrypt the cipher text only if the set of attributes of the user key matches the attributes of the cipher text. An important feature in such type of encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. Several settings are there where a user would want to give access to documents based on certain position/role of a person. We would want different kind of users of the database to be able to see only those contents that are relevant to them. Similarly, in a distributed setting where all the data may be stored in a server, the server might allow access to files and documents based on some predefined access control policy, for instance, clients may have to provide proper certification to retrieve specific files.

If the data (storage) in the database or server is compromised, then although it may be in the encrypted form, anyone who has access to the database or server may be able to retrieve all information including those documents that may not be relevant to them. It provides a mechanism by which we can ensure that even if the storage is compromised, the loss of information will only be minimal. What it does is that, it effectively binds the access-control policy to the data and the users (clients) instead of having a server mediating access to files.

An access control policy would be a policy that defines the kind of users who would have permissions to read the documents. E.g. In an academic setting, grade-sheets of a class may be accessible only to a professor handling the course and some teaching assistants (TAs) of that course. We will call the various credentials (or variables) of the predicate as

attributes and the predicate itself which represents the access policy as the access-structure. In the example here the access structure is quite simple. But in reality, access policies may be quite complex and may involve a large number of attributes.

There are two major features to Peculiarity based encryption. Firstly it has the capacity to address complex access control policies. Secondly the exact list of users need not be known apriori. Knowledge of the access Policy is sufficient. Also, an important property that these schemes must satisfy is that of collusion resistance which means that, if 2 or more users possessing different keys combine to decrypt the cipher text, they will be successful if and only if any one of the users could have decrypted it individually. In other words, even if multiple parties collude, they should not be able to decrypt the cipher text unless one of them was able to decrypt it completely by herself. These properties ensure that only users possessing the right keys have access to the information. Moreover, as the encryption is based on the access-structure it implicitly assures anonymous access control.

Contribution

In most of the previous ABE schemes, the size of the cipher text is very large, it is usually in the order of the number of attributes under consideration .the current constant size cipher text schemes are applicable only to some restricted access structures and even the most efficient scheme with expressive access control has cipher text size proportional to the number of attributes involved .In this we propose an approach to get a multi-level threshold where the cipher text size is independent of the number of attributes. Moreover, the access structure we use is more expressive and can be used to represent complex access control policies.

CONSTRUCTION

It is a new encryption scheme where an identity is seen as a set of attributes. In this a user can access to some resources only if she had a set of attributes satisfying a control access policy previously defined. The policy is described through a Boolean formula, which can be represented by an access structure and can be implemented using a linear secret-sharing scheme (LSSS). The LSSS structure is described by the pair (M, p), where M belongs to F is an u × t matrix, where u, t are the number of required attributes, whereas p is a label function that according to the policy links each row of the matrix M to an attribute. We reformulate the protocol from its original symmetric setting to an asymmetric one where some scheme parameters are conveniently defined in G1 whereas others are in G2. The scheme is made up of four algorithms:

Setup

The security parameter λ as input and the set of U attributes. The security parameter becomes the main criterion to select the groups G1 and G2 of order r and the generators P€G1 and Q€G2. The points H1…….HU € G1 are generated from the attribute universe and the algorithm also chooses two random integers a, α € Fr. the authority establishes MSK = [α] P as her master secret key This algorithm has a cost of one pairing, two scalar multiplications and U Map To Point functions. It is assumed that the elements P, Q, [α] P and e (Q, P) ^α are all known in advance. On the contrary, the points H1…..HU were not considered as fixed points since the attribute universe has a variable length, a fact that is also reflected in the storage cost.

Encrypt

It takes public key PK as input, the message M to be encrypted, and the LSSS access structure (M, p), where

M belongs to Fr is a u × t matrix as described above. The algorithm starts by randomly selecting a column vector v = (s; y2…….yt) ^T € Fr that will be used to securely share the secret exponent s. For i = 1 to u, it calculates yi = Mi .v where Mi is the 1 X t vector corresponding to the i-th row of M. The scalars r1…….. ru € Fr are also randomly chosen. Then, the cipher CT is published as follows:

C = {Me (QP) ^αs, C' = [s] Q}

This is sent along with the LSSS access structure (M, p). The comb method was applied to compute scalar multiplications involving the fixed points Q, P and [a] P. In the same way, one can apply this method to obtain the powering of e (Q, P) ^α by the exponent s. The GLV method was used to compute scalar multiplications with the points Hi € G1. Hence the cost of encryption is one multiplication and one fixed exponentiation in GT, u fixed point multiplications in G1, u + 1 fixed point multiplications in G2 and u point multiplication in G1.

Key Generation

It takes as input the master secret key MSK = αP and a set of attributes S. First the algorithm selects a random number t € Fr, then it generates the private key as follows,

SK = {K = [α] P + [t] ([α] P); L = [t] Q, ɣx€ S Kx = [t] Hx}

Let N be the number of attributes on S, since the points αP and Q are known, the cost of this algorithm is one fixed point multiplication in G1, one fixed point in G2 and N point multiplications in G1. For the first two scalar multiplications the comb method was used, and the GLV method for the rest.

Decrypt

It takes cipher CT as input with the access structure(M, p) and the private key SK for a set S. Suppose S satisfies the access structure and define I C {1, 2…. u} as I = {i : p(i) € S}. Let {wi €Z} i€I be the set of constants P such that if λi is a valid share of a secret s according to M.The decryption algorithm first computes:

Dec (CT, SK, PK)

E (L,[wi]Ci)πe(Di, [wi] Kp(i))/e (C',K) = e(P;Q)αs;

Followed by the multiplication of this value by C, If S satisfies the access structure this should recover the message M.

RELATED WORK

The cipher text policy ABE scheme developed by Bethencourt, which was based on secret sharing, was actually a scheme that supported multi-level threshold access structures. The scheme was developed in a manner which could very easily be extended to support generic access structure by simply replacing any AND by n-out-of-n threshold gate and an OR by 1-out-of-n threshold gate. Later, the work by Ostrovsky gave a key policy based scheme that extended to non-monotone access structures. In order to give this schemes other properties, including better security, the simple AND access structure became more popular the use of the simple AND based access structure was also used to develop schemes that gave more efficient cipher text size. All the initial encryption schemes, both Key policy based and Cipher text policy based had cipher text size and key size in the order of atleast the number of attributes involved. The first attempt to make the most efficient cipher text policy attribute based encryption can be credited to Waters. Here he proposes a scheme, in

which the size of the cipher text is equal to the number of attributes involved; recently, the work by Herranz proposes an elegant scheme for a constant cipher text size threshold. Their work makes use of a clever aggregate method proposed by Delerablee and Pointcheval. Although the threshold scheme is more expressive, the aggregate function is useful as long as there is only one level in the access structure and does not seem to be easily extendible to the multi-level threshold case.

In this work we make use of the Aggregate function to obtain a more expressive multi-level threshold which is also efficient with respect to the size of the cipher text and the number of pairing operations involved.

CONCLUSIONS

We focused on cipher text-policy based schemes since the access policy is associated with the cipher text during encryption and each user gets keys based on the attributes/credentials they have We paid particular attention to efficiency because, almost all attribute-based solutions require a huge number of components for keys and cipher text, making them cumbersome for large-scale tasks. Although some constant-size threshold schemes exist, they only support one gate and are not as expressive as some of the applications and real-world situations require them to be. Ours is an attempt to give an efficient scheme that does not compromise on the expressiveness of the access policy. We leave it as an open problem to come up with a provably secure attribute based signature scheme with a key construct that makes use of the linear secret sharing scheme combined with Waters' signature. We looked at attribute-based signatures, and pointed out vulnerabilities in a number of schemes. We closely examined the key-generating algorithm on which our attacks were based. Then, we formally presented the different kind of ways in which each of these schemes could be attacked. We concluded that the attacks cannot be fixed easily just by changing the number of components (attributes and dummies) given to the user; a fix would require a different key generating mechanism altogether. But we still think it is a worthwhile venture to design a threshold based signature scheme built on Waters' signature and secret sharing principle that is resistant to our attack.

REFERENCES

1. Amit Sahai and Brent Waters, Fuzzy Identity-Based Encryption
2. Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
3. Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
4. David Lubicz and Thomas Sirvent, Attribute-Based Broadcast Encryption Scheme Made Efficient
5. Ari Jules and Michael Szydlo, Attribute-Based Encryption: Using Identity-Based Encryption for Access Control
6. D. Halevy and A. Shamir. The LSD Broadcast Encryption Scheme. In Advances in Cryptology – CRYPTO, volume 2442 of LNCS, pages 47–60. Springer, 2002.
7. Hugh Harney, Andrea Colgrove, and Patrick Drew McDaniel. Principles of policy in secure groups. In NDSS, 2001.
8. Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. In Lars R. Knudsen, editor